CLAIMS

What is claimed is:

1. A method for redirecting network message traffic comprising

receiving an indication of undesirable message traffic directed to a particular target node via a first transport mechanism in a communications network;

rerouting all message traffic carried via the first transport mechanism in the communications network, and directed to the particular target node, to a filter complex operable to distinguish desirable message traffic from undesirable message traffic; and

directing the filtering complex to transmit, via a second transport mechanism over the communications network, the desirable message traffic to the target node.

2. The method of claim 2 further comprising directing the filtering complex to filter the message traffic to subdivide desirable message traffic from undesirable message traffic.

3. The method of claim 1 wherein the filter complex further comprises a security filter having filtering logic for performing filtering, the security filter operable to parse the message traffic and identify sequences in the message traffic indicative of undesirable message traffic.

4. The method of claim 3 wherein the filter complex further includes a filter routing device in communication with other routing devices in the communications network and coupled to the security filter for analyzing message traffic.

5. The method of claim 4 wherein the filter routing device in the filtering complex is operable to communicate according to the first transport mechanism and the second transport mechanism.

6. The method of claim 1 wherein the rerouting all message traffic includes directing the filter complex from a network management server in communication with the filter

complex, the network management server operable to send a reroute message to the filtering complex.

7. The method of claim 1 wherein directing further comprises directing a target node router serving the target node from the network management server, the network management server operable to send a redirect message to the target node router.

8. The method of claim 6 wherein the reroute message is indicative of the filtering complex receiving message traffic according to the first transport mechanism intended for the target node via the target node router serving the target node.

9. The method of claim 7 wherein the redirect message is indicative that the target router serving the target node is not to receive message traffic according to the first transport mechanism corresponding to the target node.

10. The method of claim 7 wherein the redirect message is indicative that the target node router serving the target node receives the desirable message traffic in the second transport mechanism corresponding to the target node.

11. The method of claim 1 wherein first and second transport mechanisms coexist on a common physical network.

12. The method of claim 1 wherein first transport mechanism corresponds to a public access protocol adapted for communication via a plurality of dissimilar network switching devices.

13. The method of claim 1 wherein the second transport mechanism corresponds to a virtual private network operable to encapsulate message packets of dissimilar protocols such that the encapsulated message packets are recognized by a routing protocol of the virtual private network.

14. The method of claim 1 wherein rerouting all message traffic further comprises propagating, via a standard protocol corresponding to the first transport mechanism, a node address other than the node address corresponding to the target node.

15. The method of claim 1 wherein directing the filter complex further comprises propagating routing information according to a predetermined protocol, the routing information operable to designate the target node as the destination of the message according to the second transport mechanism.

16. The method of claim 1 wherein rerouting all message traffic is a static route, according to the first transport mechanism, from a single router serving the target node to the filter router serving the filter complex.

17. The method of claim 1 wherein receiving an indication further comprises detecting a pattern of undesirable message traffic in quantity sufficient to be recognized.

18. The method of claim 1 wherein the undesirable message traffic emanates from a plurality of sources, each of the plurality of sources independently contributing substantially insignificant volume of message traffic.

19. A network management server for redirecting undesirable message traffic comprising:

a network intrusion detector monitor operable to receive an indication of undesirable message traffic directed to a particular target node via a first transport mechanism in a communications network;

a routing processor operable to propagate routing information to reroute all message traffic using the first transport mechanism directed to the particular target node; and

a filter complex responsive to the rerouting processor, the filter complex operable to distinguish desirable message traffic from undesirable message traffic, and further

operable to transmit, via a second transport mechanism over the communications network, the desirable message traffic to the target node.

20. The network management server of claim 19 wherein the filtering complex is further operable to filter the message traffic to subdivide the desirable message traffic from the undesirable message traffic.

21. The network management server of claim 19 wherein the filter complex further comprises a security filter having filtering logic for performing filtering, the security filter operable to parse the message traffic and identify sequences in the message traffic indicative of undesirable message traffic.

22. The network management server of claim 21 wherein the filter complex further includes a filter routing device in communication with other routing devices in the communications network and coupled to the security filter to analyze message traffic.

23. The network management server of claim 12 wherein the filter routing device in the filtering complex is operable to communicate according to the first transport mechanism and the second transport mechanism.

24. The network management server of claim 19 wherein the network management server is operable to send a reroute message to the filtering complex, in response to which the filter complex is operable to reroute the message traffic.

25. The network management server of claim 19 wherein the routing processor is further operable to direct a target node router serving the target node from the network management server, the network management server operable to send a redirect message to the target node router.

26. The network management server of claim 24 wherein the routing processor is further operable to send a reroute message is indicative of the filtering complex receiving

message traffic accordance to the first transport mechanism intended for the target node via the target node router serving the target node.

27. The network management server claim 25 wherein the routing processor is further operable to send a redirect message indicative that the target router serving the target node is not to receive message traffic according to the first transport mechanism corresponding to the target node.

28. The network management server claim 25 wherein the redirect message from the routing processor is further indicative that the target node router serving the target node receives the desirable message traffic in the second transport mechanism corresponding to the target node.

29. The network management server of claim 19 wherein a network interface in the network management server is compatible with the first and second transport mechanisms and wherein first and second transport mechanisms coexist on a common physical network.

30. The network management server of claim 19 wherein first transport mechanism is operable according to a public access protocol adapted for communication via a plurality of dissimilar network switching devices.

31. The network management server of claim 19 wherein the second transport mechanism is operable according to a virtual private network protocol operable to encapsulate message packets of dissimilar protocols such that the encapsulated message packets are recognized by a routing protocol of the virtual private network.

32. The network management server of claim 19 wherein the filter complex is operable to reroute all message traffic including propagating, via a standard protocol corresponding to the first transport mechanism, a node address other than the node address corresponding to the target node.

33. The network management server of claim 19 wherein the routing processor is operable to direct the filter complex to propagate routing information according to a predetermined protocol, the routing information operable to designate the target node as the destination of the message according to the second transport mechanism.

34. The network management server 1 wherein the routing processor is operable to rerouting the message traffic according to a static route in the first transport mechanism, from a single router serving the target node to the filter router serving the filter complex.

35. The network management server of claim 19 wherein the undesirable message traffic emanates from a plurality of sources, each of the plurality of sources independently contributing substantially insignificant volume of message traffic.

36. In a network management server of a networked system of data communications devices, a method for transparently intercepting, filtering, and rerouting message traffic for recovering from a distributed denial of service attack comprising:

detecting, at a network monitor in the network management server, a pattern of inundating undesirable message traffic to a particular target node transported via a first transport mechanism in a communications network;

receiving, via a routing processor, an indication of the undesirable message traffic directed to the particular target node;

transmitting, via a network interface, a reroute message to a filter complex having a security filter operable to distinguish desirable message traffic from undesirable message traffic; and

rerouting, via a filter routing device in the filter complex, all message traffic carried via the first transport mechanism in the communications network and directed to the particular target node;

filtering, at the security filter, the message traffic to bifrucate desirable message traffic from undesirable message traffic;

transmitting, via the network interface to a target node router serving the target node, a redirect message indicating that the target node router is to receive, via the second transport mechanism, the desirable message traffic directed to the particular target node and rerouted to the filter complex, the filter complex and the target node router conversant in the first transport mechanism and the second transport mechanism; and

directing, from the network management server, the filtering complex to transmit, via a second transport mechanism over the communications network, the desirable message traffic to the target node.

37. A computer program product having a computer readable medium operable to store computer program logic embodied in computer program code encoded thereon for for redirecting network message traffic comprising:

computer program code for receiving an indication of undesirable message traffic directed to a particular target node via a first transport mechanism in a communications network;

computer program code for rerouting all message traffic carried via the first transport mechanism in the communications network and directed to the particular target node, to a filter complex operable to distinguish desirable message traffic from undesirable message traffic; and

computer program code for directing the filtering complex to transmit, via a second transport mechanism over the communications network, the desirable message traffic to the target node.

38. A computer data signal embodying program code for redirecting network message traffic comprising:

program code for receiving an indication of undesirable message traffic directed to a particular target node via a first transport mechanism in a communications network;

program code for rerouting all message traffic carried via the first transport mechanism in the communications network and directed to the particular target node, to a filter complex operable to distinguish desirable message traffic from undesirable message traffic; and

program code for directing the filtering complex to transmit, via a second transport mechanism over the communications network, the desirable message traffic to the target node.

39. A network management server for redirecting undesirable message traffic comprising:

means for receiving an indication of undesirable message traffic directed to a particular target node via a first transport mechanism in a communications network;

means for rerouting all message traffic carried via the first transport mechanism in the communications network and directed to the particular target node, to a filter complex operable to distinguish desirable message traffic from undesirable message traffic; and

means for directing the filtering complex to transmit, via a second transport mechanism over the communications network, the desirable message traffic to the target node.